UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/879,575	06/12/2001	James Alexander Reeds III	1999-0275	4755

34700 7590 04/27/2006

ZAGORIN OBRIEN GRAHAM LLP
7600B N. CAPITAL OF TEXAS HWY
SUITE 350
AUSTIN, TX 78731

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 04/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/879,575	REEDS ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-53* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-53* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: filed on 14 November 2005 with acknowledgement of an original application filed on 12 June 2001.

2. Claims 1-53 are currently pending in this application. Claims 1, 14, 33, 41, 48, 49, and 53 are independent claims, no amendment to the claims has been proposed.

Response to Arguments

3. Applicant's arguments filed 14 November 2005 have been fully considered but they are not persuasive.

In response to applicant's argument on page 16, "The arguments regarding the non-statutory subject matter of the previous response are hereby incorporated by reference, and apply to all claims... {***from the previous remarks 'all claims are directed to a specific hardware device which can utilize software component'***}... The Examiner's rejection under § 101 is unfounded, and completely without basis in statutory or common". The Office does not agree the 101 rejection is maintained because the applicant has not provided enough detail in the claims how a person of ordinary skill in the art would use the invention and what steps are needed to perform the invention or improvement expected by using the invention. Furthermore as stated in previous rejection "***the applicant is claiming apparatus such as a receiver or a transmitter utilizing the method of a software program. To overcome this rejection the applicant needs to amend the claims so that the language in the body of the claims links the apparatus to perform an operation***".

In addition as per Office Guidelines, the Examiner arrives at this 101 rejection because:

The non-statutory subject matter is an abstract idea that does not have a practical application because 'the selection of a fixed length segment of a continuous decryption key stream based on a received session count of a data packet' is not a constant or concrete step. Although the claim indicates 'fixed length segment' nothing that contributes to this fixed length segment is fixed, a key stream is not constant, the received session count, is a number that changes with each session, therefore it is not fixed. The idea of selected a fixed length from a stream based on a number that is incremented with each session does not provide concrete repeatable results and therefore it is not patentable.

In formulating this 101 rejection the examiner does not find that the claims transform the article, i.e. the computer, transceiver, or receiver is not changed. Therefore the examiner reviewed the claims to determine if the claims provide a practical application that produces a useful, tangible and concrete result. Of these three tests the examiner finds the claims fail the tangible and concrete result test.

In determining whether the claim is for a "practical application," the focus is not on whether the steps taken to achieve a particular result are useful, tangible and concrete, but rather that the final result achieved by the claimed invention is "useful, tangible and concrete."

In determining whether a claim provides a practical application that produces a useful, tangible, and concrete result, the examiner finds the claims are not a "TANGIBLE RESULT"

The tangible requirement does not necessarily mean that a claim must either be tied to a particular machine or apparatus or must operate to change articles or materials to a different state or thing. However, the tangible requirement does require that the claim must recite more than a § 101 judicial exception, in that the process claim must set forth a practical application of that

§ 101 judicial exception to produce a real-world result. The claims do not produce a real-world result because they are trying to provide a decryption method based on data received that is not constant and that has not been previously defined.

In determining whether a claim provides a practical application that produces a useful, tangible, and concrete result, the examiner finds the claims are not a "CONCRETE RESULT".

Another consideration is whether the invention produces a "concrete" result. Usually, this question arises when a result cannot be assured. In other words, the process must have a result that can be substantially repeatable or the process must substantially produce the same result again. In re Swartz, 232 F.3d 862, 864, 56 USPQ2d 1703, 1704 (Fed. Cir. 2000) (where asserted result produced by the claimed invention is "irreproducible" claim should be rejected under section 101). The opposite of "concrete" is unrepeatable or unpredictable. Resolving this question is dependent on the level of skill in the art. For example, if the claimed invention is for a process which requires a particular skill, to determine whether that process is substantially repeatable will necessarily require a determination of the level of skill of the ordinary artisan in that field. Because session counts and a key streams are always changing a method for decryption is changing. Therefore the claimed invention is not concrete.

In response to applicant's argument on page 17, "Claims 1-53 were rejected under 35 U.S.C. §112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which application regards as the invention. All independent claims contain the phrase "fixed length segment" followed by using "a portion of the fixed length segment" however, there is no indication how this portion is selected and no further

description of a fixed length segment. Those skill in the art will understand the plain meaning of these words. A fixed length segment is a segment having a fixed length, as opposed to one having a variable length, and is described, for example, in paragraphs 0026-0028 ... The Examiner's confusion over the meaning of the claims is therefore not understood". The Examiner disagrees with argument, the claims are rejected for being indefinite because there is no real world application how a fixed length is selected and how it is applied, the applicant is simply claiming an abstract idea without a real world application.

In response to applicant's second argument beginning on page 17, "Claims 4, 17, 25-32, 36, and 44 were rejected as indefinite under 35 U.S.C. 112, second paragraph, for including the trademark/trade name "RC4". As the Examiner notes, MPEP 706.03(d) indicates that "When a trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112, second paragraph" ...The use of the term "RC4 operation" in these claims is not used to describe a particular material or product, and so does not fall under this prohibition ... The "opentopia" description attached by the Examiner to the Office Action clearly indicates that the RC4 cipher is well known to those of skill in the art, and even includes pseudocode for implementing the algorithm ... a copy of the relevant pages of Schneier's Applied Cryptograph (Bruce Schneier, 2nd Edition, 1996) are attached, describing the very well known (even as of 10 years ago) RC4 algorithm". The Examiner disagrees with arguments relating to the use of "RC4" in the claims, applicant is using the term RC4, RC4 is a trademark as indicated by the opentopia cited reference no matter how well known it should not be placed in the body of the claim.

In response to applicant's arguments beginning on page 19, "Medvinsky does not teach the literal term "session count" at all. Of course, this is not required, if Medvinisky uses another term that fits the usage of "session count" in the present application. Medvinsky includes no such teaching ... Medvinsky also references another, "Counter N", but this counter tracks CODEC changes, not number of packets". The Examiner disagrees with arguments for multiple reasons. The application was rejected as best understood in light of the 112 and 101 problems noted, the applicant chose to no further amend the claims. The claims as best understood indicate 'selection of a fixed length segment based on a received session count of a data packet' the claims contain too much ambiguity to differentiate what session count is referring to, a session count as best understood is a number assigned to communication received in a computer system when receiving data packets, the session count usually are incremented, with each data packet received. As argued Medvinsky shows multiple means of tracking the data packets time stamped (RTP) but also the data packets communicated are tracked, session identifier's (SSRC), the SSRC is another term for session count see paragraph 0014 on Medvinsky page 2.

In response to applicant's argument beginning on page 20, 'The Office Action states that claims 9-13, 28-32, 40, and 52 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Medvinsky over Staring ... As demonstrated above, Medvinsky does not teach a "session count" as used in the present application and found in each independent claim. Similarly, Staring has no teaching or suggestion. Staring does teach "session keys", but these are not related to packet count, as in the present application. The Examiner disagrees with argument as explained above session count is taught in Medvinsky, furthermore the session key described in Staring relates to the session as known in the art.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 1-53 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Independent claims 1, 14, 33, 41, 48, 49, and 53 are directed to a method comprising: "a session count evaluator configured" and "a decryption engine". The terminology used as well as the description in the specification indicates that the session count evaluator and the decryption engine are nothing more than a computer program or software. In order to overcome this rejection applicant must show that a component or device is needed to perform the language claimed, in addition applicant needs to show how the device or equipment is needed to perform the steps.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1-53 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. All the independent claims contain the phrase "fixed length segment" followed by using " a portion of the fixed length segment" there is not any indication how this portion is selected and there is no further description of a fixed length segment.

8. Claims 4, 17, 25-32, 36, and 44 contain the trademark/trade name "RC4" owned by RSA. Where a trademark or trade name is used in a claim as a limitation to identify or describe a

particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112, second paragraph. See *Ex parte Simpson*, 218 USPQ 1020 (Bd. App. 1982). The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. A trademark or trade name is used to identify a source of goods, and not the goods themselves. Thus, a trademark or trade name does not identify or describe the goods associated with the trademark or trade name. In the present case, the trademark/trade name is used to identify/describe a proprietary standard for stream cipher and, accordingly, the identification/description is indefinite. As discussed previously RC4 is a trademark it should not be in the claims. The applicant can overcome this rejection by providing a specification of RC4 algorithm.

9. To expedite a complete examination of the instant application the claims rejected under 35 U.S.C. 101 (nonstatutory) as well as 35 U.S.C. 112 above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11. **Claims 1-8, 14-27, 33-39, 41-51, and 53** are rejected under 35 U.S.C. 102(e) as being anticipated by Medvinsky U.S. Patent Application Publication No. 2002/0094081 (hereinafter '081).

As to independent claim 1, "A method comprising: selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet" is taught in '081 pages 3-4 paragraphs 0033-0034;

"and decrypting a payload of the data packet by applying a portion of the fixed length segment to the data packet" is shown in '081 page 2, paragraphs 0017-0018.

As to dependent claim 2, "wherein the applying comprises performing a bit per bit streaming encryption process" is disclosed in '081 page 3, paragraph 0034.

As to dependent claim 3, "wherein the applying further comprises performing an exclusive OR operation with the portion of the fixed length segment and the data packet" is taught in '081 page 3, paragraph 0034.

As to dependent claim 4, "wherein the applying further comprises performing an RC4 operation with the portion of the fixed length segment and the data packet" is shown in '081 page 3, paragraph 0034.

As to dependent claim 5, "further comprising: receiving the data packet, the data packet comprising at least a portion of the received session count" is shown in '081 page 2, paragraphs 0017-0018.

As to dependent claim 6, "wherein the data packet further comprise at least a portion of a received message digest value" is disclosed in '081 page 4, paragraph 0054.

As to dependent claim 7 "wherein the selecting comprises: selecting a current fixed length segment if a difference between the received session count and a locally generated session count is less than a threshold value" is shown in '081 page 4, paragraphs 0036-0051.

As to dependent claim 8, "wherein the selecting further comprises: extracting the at least a portion of the received session count from the encrypted data packet; expanding the at least a portion of the received session count to the received session count; and comparing the received session count to the locally generated session count" is disclosed in '081 pages 3-4 paragraphs 0033-0034.

As to independent claim 14, "A method of generating an encrypted data packet, the method comprising: selecting a fixed length segment of a continuous encryption key stream" is taught in '081 pages 3-4 paragraphs 0033-0034;

"applying a portion of the fixed length segment to data to form an encrypted payload; generating a session count based in accordance with the fixed length segment; and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet" is shown in '081 page 2, paragraphs 0017-0018.

As to dependent claims 15, 16, and 17, these claims contain substantially similar subject matter as claims 2, 3, and 4; therefore they are rejected along the same rationale.

As to dependent claim 18, "further comprising: generating a message digest value; and combining at least a portion of the message digest value with the encrypted payload to form the encrypted data packet" is taught in '081 page 4, paragraphs 0054 –0055.

As to dependent claim 19, "wherein the generating comprises: generating the message digest value based on the encrypted payload, the session count and a message digest key" is shown in '081 page 4, paragraphs 0054 –0055.

As to dependent claim 20, "further comprising: forming the at least a portion of the message digest value by truncating the message digest value" is disclosed in '081 page 4, paragraphs 0054 –0055.

As to dependent claim 21, "further comprising transmitting the encrypted data packet to a receiver through a communication channel" is taught in '081 page 2, paragraph 0016.

As to dependent claim 22, "further comprising: receiving a received data packet corresponding to the encrypted data packet, the received data packet comprising the encrypted payload, at least a portion of a received session count and a received truncated message digest value; selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet; and decrypting a payload of the data packet by applying a portion of the fixed length segment to the data packet" is shown in '081 pages 3-4 paragraphs 0033-0034 and page 4, paragraphs 0053-0055.

As to dependent claims 23-27, these claims contain substantially similar subject matter as claims 2-8; therefore they are rejected along the same rationale.

As to independent claim 33, "A receiver comprising: a session count evaluator configured to determine if a difference between a received session count within a received encrypted data packet and a locally generated session count is less than a threshold" is taught in '081 pages 3-4 paragraphs 0033-0034;

"and a decryption engine configured to decrypt a payload of the received encrypted data packet by applying a portion of a current fixed length segment of a continuous decryption key stream to the data packet if the difference is less than the threshold" is shown in '081 page 2, paragraphs 0017-0018.

As to dependent claims 34-39 these claims contain substantially similar subject matter as claims 2-8; therefore they are rejected along the same rationale.

As to independent claim 41, this claim is directed to a transmitter of the method of claim 14; therefore it is rejected along similar rationale.

As to dependent claims 42-51, these claims contain substantially similar subject matter as claims 2-8; therefore they are rejected along the same rationale.

As to independent claim 48, is directed to a system consisting of independent claims 33 and 41; therefore it is rejected along the same rationale.

As to independent claim 49, "A method comprising: receiving a data packet through a communication channel" is taught in page 2, paragraph 0016;

"the data packet comprising at least a portion of a session count; selecting a fixed length segment of a continuous decryption key stream based on the session count" is taught in '081 pages 3-4 paragraphs 0033-0034;

"and applying a portion of the fixed length segment by performing a bit per bit streaming encryption to decrypt a payload of the data packet" is shown in '081 page 2, paragraphs 0017-0018.

As to dependent claims 50 and 51, these claims contain substantially similar subject matter as claims 7 and 8; therefore they are rejected along the same rationale.

As to independent claim 53, **"A method of generating an encrypted data packet, the method comprising: selecting a fixed length segment of a continuous encryption key stream"** is taught in '081 pages 3-4 paragraphs 0033-0034;

"applying a portion of the fixed length segment to data by performing a bit per bit streaming encryption process to form an encrypted payload; generating a session count in accordance with the fixed length segment; and combining the encrypted payload and the at least a portion of the session count to form an encrypted data packet" is shown in '081 page 2, paragraphs 0017-0018.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 9-13, 28-32, 40, and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over '081 in further view of Chang et al. U.S. Patent 6,105,012 (hereinafter '012).

As to dependent claim 9, "further comprising: discarding the data packet if the difference is not less than the threshold value" however '012 teaches "The key check block is sent to the receiver as a header of the current encrypted data payload. The receiver also retains the last eight bytes of the current packet, it decrypted the first eight bytes (the key check block) and compares the result to the retained last eight bytes ... If there is no match, an error occurred and the receiver takes appropriate action" on page 5, paragraph 0052.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method key selection for decryption taught in '081 to include a means to compare the keys being used and take appropriate action (i.e. delete packet) when a match is not found. One of ordinary skill in the art would have been motivated to perform such a modification because of the need to protect data during transmission see '012 (page 1, paragraphs 0005-0006). "It is known to remedy this deficiency by decrypting the data field of the packet with the current session key, as well as the next key in the sequence of keys, and choose the key for which the decrypted data makes sense. Using this method, the change-over from one session key to the next is automatically detected. However, to determine whether the decrypted data makes sense requires knowledge about the information being transmitted. This is not always the case, limiting the use of this method. It is an object of the invention to provide a secure communication system, sink device and secure communication method which overcome above mentioned drawback".

As to dependent claim 10, "further comprising: re-synchronizing a decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the difference in not less than the threshold value" is taught in '081 page 4, paragraphs 0041- 0053 "it signals the CODEC change to gateway controller 106. MTA 104 generates a new set of RTP key stream and a new initial time stamp. Herein lies a first advantage of the present invention. The related art provides for re-derivation of the RTP key stream when a CODEC change occurs, by providing the following key derivation function ... "End-End RTP Key Change <N>" is a label that is used as a parameter to the key derivation function".

As to dependent claim 11, "further comprising: discarding the data packet if the at least a portion of the received message digest value does not match a locally generated message digest value" is taught in '012 page 5, paragraph 0052-0053.

As to dependent claim 12, "further comprising: re-synchronizing the decryption key to an encryption key by setting the decryption key and the encryption key to a start vector if the at least a portion of the received message digest value does not match the locally generated message digest value" is shown in '081 page 4, paragraph 4-5, paragraphs 0054-0057 "In a further embodiment, the above solution is employed for a MAC (Message Authentication Code) algorithm change, resulting in a packet size change. Traditionally, for convenience the same RC4 key stream may be used in the generation of the keying material needed to calculate a MAC for each packet (a MAC is appended after the encrypted text). Where the MAC pad is key used to generate the MAC, for one-time use only. So, wehre a key stream is used for MAC generation (instead of or in addition to encryption) and the size of that random pad changes, one must rekey and start a new RC4 key stream in the same way as fro CODE changes".

As to dependent claim 13, "further comprising: extracting the at least a portion of the received message digest value from the data packet; generating the locally generated message digest value based on the at least a portion of the received session count, a received encrypted payload of the data packet and a message digest key; truncating the locally generated message digest value to form a truncated message digest; and comparing the truncated message digest to the at least a portion of the received message digest value" is shown in '081 page 4, paragraph 4-5, paragraphs 0054-0057.

As to dependent claims 28-32, these claims contain substantially similar subject matter as claims 9-13; therefore they are rejected along the same rationale.

As to dependent claim 40, "further comprising: a message digest extractor configured to extract the at least a portion of the received message digest value from the received encrypted data packet" is taught in '081 page 4, paragraph 0054 "In a further embodiment, the above solution is employed for a MAC (message Authentication Code) algorithm change, resulting a in a packet size change";

"a message digest generator configured to generate a locally generated message digest value based on the at least a portion of the session count, a received encrypted payload of the data packet and a message digest key" is shown in '081 pages 4-5 paragraph 0055-0056 "For example, additional key stream bytes may be allocated to calculate a MAC for each frame. However, ehre is only one MAC needed for the whole RTP packet and if an RTP packet contains multiple frames only the key stream bytes allocated to one of the frames ... Where the MAC pad is a key used to generate the MAC, for one-time use only;

"a truncator configured to truncate the locally generated message digest value to form a truncated message digest; and a message digest evaluator configured to compare the truncated message digest value to the at least a portion of the received message digest value" is disclosed in '081 page 5, paragraph 0057 "one must rekey and start a new RC4 key stream in the same way as fro CODEC changes";

"where the received is configured to discard the received encrypted data packed it the truncated message digest value does not match the at least a portion of the received message digest value" is taught in '012 page 5, paragraph 0052 "The key check block is sent to

the receiver as a header of the current encrypted data payload. The receiver also retains the last eight bytes of the current packet, it decrypted the first eight bytes (the key check block) and compares the result to the retained last eight bytes ... If there is no match, an error occurred and the receiver takes appropriate action".

As to dependent claim 52, "further comprising discarding the data packet if the difference is not less than the threshold value" is taught in '012 page 5 paragraph 0052.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 2:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ECT

Ellen Tran
Patent Examiner
Technology Center 2134
24 April 2006